UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,412	12/21/2001	Alex J. Hinchliffe		3596

7590 02/26/2009

Zilka-Kotab PC
PO Box 721120
San Jose, CA 95172-1120

EXAMINER	
DENNISON, JERRY B	
ART UNIT	PAPER NUMBER
2443	

MAIL DATE	DELIVERY MODE
02/26/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ALEX J. HINCHLIFFE, ANDREW KEMP,
BOBBY RAI, and FRASER P. HOWARD

Appeal 2008-2948
Application 10/028,412
Technology Center 2100

Decided:[1] February 26, 2009

Before JAMES D. THOMAS, JOHN C. MARTIN, and
ALLEN R. MACDONALD, *Administrative Patent Judges.*

MARTIN, *Administrative Patent Judge.*

DECISION ON APPEAL

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from
(Continued on next page.)

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1, 2, 4, 5, 7, 9-16, 18, 19, 21, 23-30, 32, 33, 35, and 37-49, which are all of the pending claims.

We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

A. Appellants' invention

Appellants' invention relates generally to computer security and more particularly to securing a desktop computer operating in a peer-to-peer network. Specification [0001].

Appellants' Figure 1 is reproduced below.

---

the Mail Date (paper delivery) or Notification Date (electronic delivery).

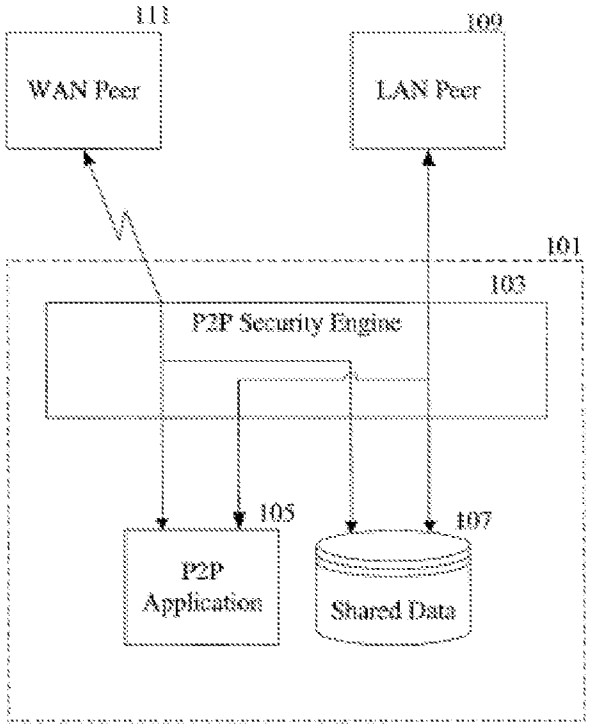

Figure 1

Figure 1 is a diagram illustrating a system-level overview of an embodiment of the invention, which includes a desktop computer 101 connected into internal and external peer-to-peer (P2P) networks. *Id.* at [0013]. The computer 101 executes a P2P application 105 to establish communications with an external WAN (wide area network) peer computer 111 or an internal LAN (local area network) peer computer 109. *Id.* The user of computer 101 has configured the computer 101 to shared data 107 (also referred to as "shares"), such as directories and files. *Id.*

A P2P security engine 103, such as a software firewall, executes on the computer 101 and monitors activity in the peer-to-peer networks, including network traffic between the computer 101 and the peers 109, 111, and file sharing on the computer 101. *Id.* The P2P security engine 103 is configured through a set of local rules that define suspicious patterns of activity and the action taken by the engine 103 if it detects such suspicious activity in the peer-to-peer network. *Id.*

The Specification provides several examples of local rules that define suspicious patterns of activity. One such local rule is to specify that all accesses to computer 101 by external peers, such as peer 111, will be logged. *Id.* at [0014]. The independent claims are specifically directed to the following "shares and permissions" example:

> [0015] The P2P security engine 103 also may be configured through rules or input parameters to record the shares and associated permissions on the computer 101. Furthermore, a baseline of authorized shares and permissions can be established on the computer 101 and a local rule defined that causes the P2P security engine 103 to log or alert when it detects changes to the baseline.

Id. at [0015].

As shown in the flowchart depicted in Figure 2, a share configuration loop (211) detects changes to shares and/or corresponding permissions on the host computer and takes appropriate action (213). *Id.* at [0022]. The action taken depends on the type of changes made and may be defined in the rules or in other input parameters. *Id.* For example, if the change is to un-

share a file or directory, thus reducing the vulnerability of the host computer to attack, a log entry may be made. *Id.*

In another embodiment, not illustrated, the share configuration loop examines the current share configuration against a previously recorded configuration, such as the baseline configuration described above, to determine if changes have been made and, if so, to determine the appropriate action to take. *Id.*

B. The claims

The independent claims before us are claims 1, 15, and 29, of which claim 1 reads:

> 1. A computerized method comprising:
>
> monitoring a peer-to-peer network for suspicious activity based on patterns of activity; and
>
> performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network;
>
> wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network;
>
> wherein a pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data;
>
> wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in

> the peer-to-peer network, the change being made with respect to the baseline.

Claims App., Br. 20.[2]

Claim 15 recites a computer readable medium having executable instructions to cause a processor to perform a method including steps identical to those recited in claim 1.

Claim 29 is a "system" claim that recites a processor and a network interface for performing functions like those recited in method claim 1.

C. The references and rejections

The Examiner relies on the following references:

Welch et al. (Welch)	US 5,862,335	Jan. 19, 1999
Conklin et al. (Conklin)	US 5,991,881	Nov. 23, 1999
Meadway et al. (Meadway)	US 6,675,205 B2	Jan. 6, 2004

Claims 1, 15, 29, and 45 stand rejected under 35 U.S.C. §112, second paragraph, for being indefinite. Answer 3.[3]

Claims 1, 2, 5, 11, 15, 16, 19, 25, 29, 30, 33, 39, and 45-49 stand rejected under § 103(a) for obviousness over Welch in view of Meadway. *Id.* at 5.

---

[2] All quotations of claim language herein are from the Claims Appendix (Br. 20-28).

[3] The rejection of claim 48 on this ground (Final Action 3) was withdrawn at page 16 of the Answer.

Claims 4, 7, 9, 10, 12-14,18, 21, 23, 24, 26-28, 32, 35, 37, 38, and 40-44 stand rejected under § 103(a) for obviousness over Welch in view of Meadway and Conklin. *Id.* at 11.

Appellants separately argue many of the rejected claims, dividing the claims that are rejected under § 112 ("Issue 1") into Groups #1 and #2 (Reply Br. 2-5), dividing the claims rejected under § 103(a) over Welch in view of Meadway ("Issue 2") into Groups #1 to #8 (*id.* at 5-15), and dividing the claims rejected over Welch in view of Meadway and Conklin ("Issue 3") into Groups #1 to #5. *Id.* at 16-20.

THE ISSUES

Appellants have the burden of showing reversible error by the Examiner in maintaining the rejections. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

The numerous specific issues raised by Appellants are identified *infra* in the discussions of the rejections.

THE § 112, SECOND PARAGRAPH REJECTION

A. Principles of law

Whether a claim is indefinite under 35 U.S.C. § 112, second paragraph, is a question of law. *IPXL Holdings LLC v. Amazon.com Inc.*, 430 F.3d 1377, 1380 (Fed. Cir. 2005).

In order to satisfy the second paragraph of § 112, the claims must "set out and circumscribe a particular area with a reasonable degree of precision and particularity." *In re Johnson*, 558 F.2d 1008, 1015 (CCPA 1977) (quoting *In re Moore*, 439 F.2d 1232, 1235 (CCPA 1971)). Furthermore, "the definiteness of the language employed must be analyzed not in a vacuum, but always in light of the teachings of the prior art and of the particular application disclosure as it would be interpreted by one possessing the ordinary level of skill in the pertinent art." *Johnson*, 558 F.2d at 1015 (quoting *Moore*, 439 F.2d at 1235).

Furthermore, the Board in *Ex Parte Miyazaki*, No. 2007-3300 (BPAI Nov. 19, 2008) (precedential), http://www.uspto.gov/web/offices/dcom/bpai/prec/fd073300.pdf at 11-12, held that "if a claim is amenable to two or more plausible claim constructions, the USPTO is justified in requiring the applicant to more precisely define the metes and bounds of the claimed invention by holding the claim unpatentable under 35 U.S.C. § 112, second paragraph, as indefinite."

B. Issue 1/Group #1 claims 1, 15, and 29

The rejection of independent claims 1, 15, and 29 is directed to the following language in each claim:

> wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network.

The Examiner concluded that the above language is unclear and indefinite in two respects. First, the Examiner concluded that the phrase "and operate substantially" is indefinite because

> [t]he term "substantially" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Answer 3, para. 1. Second, the Examiner concluded that the entire paragraph is indefinite because it "recites operating without the server, and then the limitation recites, 'by utilizing the server'. The limitation contradicts itself by reciting not using the server to connect and operate substantially, and then reciting using the server to connect and operate." *Id.* at 4, para. 2 (underlining and bolding omitted).

We agree with Appellants that the paragraph in question is clear when considered as a whole and means that "the peers, at most, use the server for providing addresses for the peers in the peer-to-peer network." Br. 9.

The § 112 rejection of claims 1, 15, and 29 is therefore reversed.

C. Issue 1/Group #2 claim 45

Turning now to the rejection of dependent claim 45, that claim reads as follows:

> 45. The computerized method of claim 1, wherein a share configuration loop is executed to detect changes to shares and corresponding permissions, and take action as a function of a type of the changes.

The Examiner concluded that this claim language is indefinite because it is "unclear to [the] Examiner what 'take action as a function of a type of the changes' means. It is also unclear as to what action is taken." Answer 4, para. 3. We agree with Appellants that this claim language is sufficiently clear. Regarding the meaning of "take action as a function of a type of the changes," the Specification (at [0015]) gives logs and alerts as examples of different actions and explains (at [0022]) that a log would be an appropriate action if the detected change is to *un-share* a file or directory. Regarding the Examiner's concern that it is unclear as to what action is taken, we agree with Appellants that it is not necessary to specifically identify the action in the claim. Br. 9.

The § 112 rejection of claim 45 is therefore reversed.

THE § 103 REJECTION (ISSUE 2) BASED
ON WELCH IN VIEW OF MEADWAY

Appellants do not challenge the combinability of the reference teachings.[4] Instead, Appellants argue that the Examiner erred in finding or concluding that various claim limitations are disclosed or suggested by the individual references.

A. Issue 2/Group #1 (Claims 1, 2, 15, 16, 29 and 30)

Of Issue 2/Group #1 claims 1, 2, 15, 16, 29, and 30, we select claim 1 for consideration. 37 C.F.R. § 41.37(c)(1)(vii).

Welch discloses a computer-implemented method of monitoring logical connections in a computer network. Welch, col. 1, ll. 47-49.

Meadway discloses a system that "performs centralized searches based on index information transmitted by peer systems to a central site

---

[4] Regarding the rejection based on Welch and Meadway, the Examiner concluded that

> it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Meadway into Welch to provide the management system of Welch with more information regarding the file transfers, by providing indexes of the contents of files that peers of the network are allowing to be shared (Meadway, col. 2, lines 10-20) in order to provide an enhanced system to diagnose problems (Welch, col. 1, lines 34-35) encountered in the computer network.

Answer 8-9.

using an agent program running on each peer, and then directs the peer systems to each other for the purpose of retrieving files." Meadway, col. 1, ll. 47-52.

The Examiner found that Welch discloses the first step of "monitoring a peer-to-peer network for suspicious activity based on patterns of activity" (Answer 5-6) and found that Meadway discloses the remaining claim limitations. *Id.* at 6-8.

Because most of Appellants' arguments are directed at Meadway, we will begin our analysis with that reference.

Figure 2 of Meadway is reproduced below.

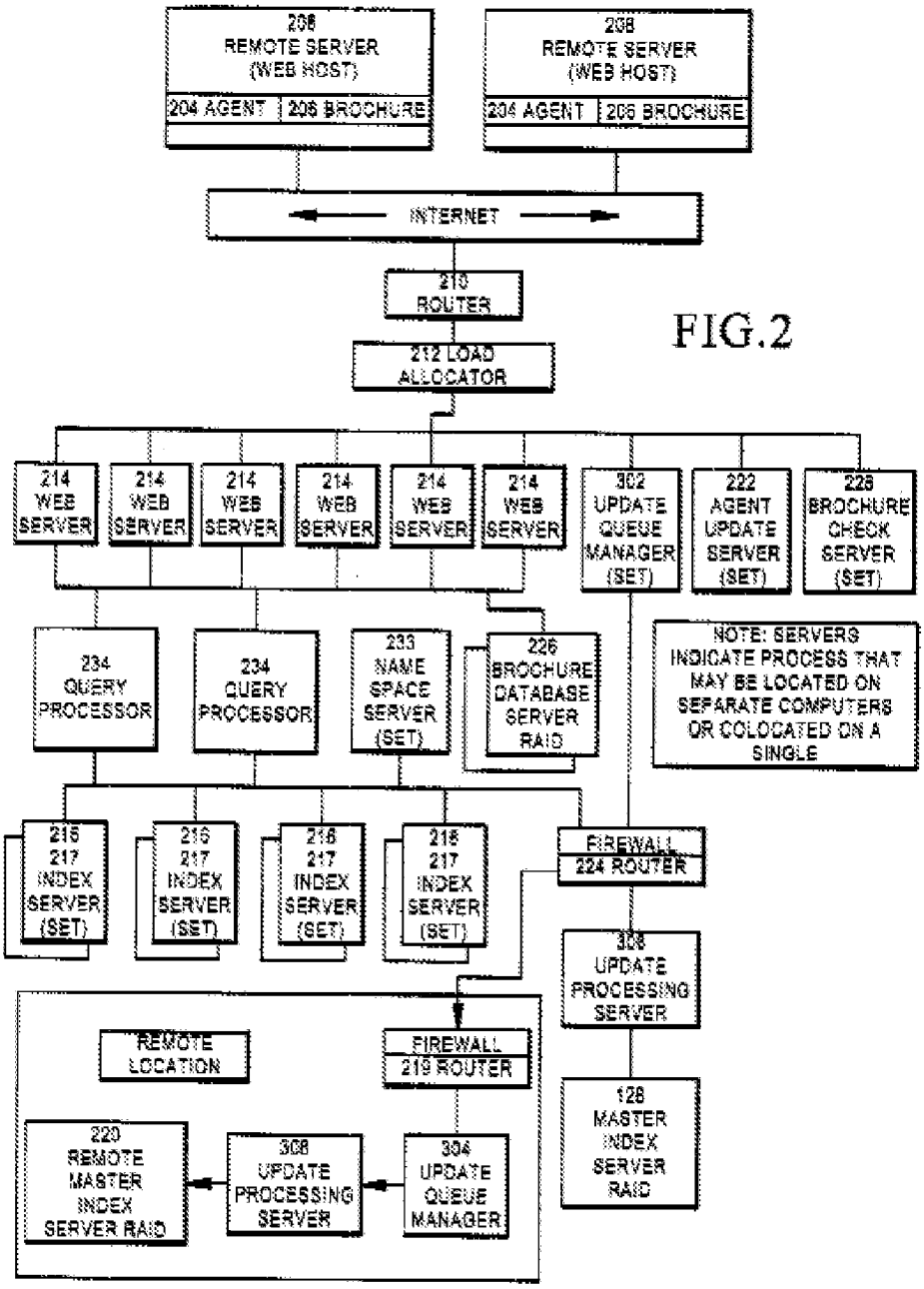
208
REMOTE SERVER
(WEB HOST)
204 AGENT
206 BROCHURE
208
REMOTE SERVER
(WEB HOST)
204 AGENT
206 BROCHURE
INTERNET
210
ROUTER
212 LOAD
ALLOCATOR
214
WEB
SERVER
214
WEB
SERVER
214
WEB
SERVER
214
WEB
SERVER
214
WEB
SERVER
214
WEB
SERVER
302
UPDATE
QUEUE
MANAGER
(SET)
222
AGENT
UPDATE
SERVER
(SET)
228
BROCHURE
CHECK
SERVER
(SET)
234
QUERY
PROCESSOR
234
QUERY
PROCESSOR
233
NAME
SPACE
SERVER
(SET)
226
BROCHURE
DATABASE
SERVER
RAID
NOTE: SERVERS
INDICATE PROCESS THAT
MAY BE LOCATED ON
SEPARATE COMPUTERS
OR COLOCATED ON A
SINGLE
216
217
INDEX
SERVER
(SET)
216
217
INDEX
SERVER
(SET)
216
217
INDEX
SERVER
(SET)
216
217
INDEX
SERVER
(SET)
FIREWALL
224 ROUTER
306
UPDATE
PROCESSING
SERVER
REMOTE
LOCATION
FIREWALL
219 ROUTER
128
MASTER
INDEX
SERVER
RAID
220
REMOTE
MASTER
INDEX
SERVER RAID
308
UPDATE
PROCESSING
SERVER
304
UPDATE
QUEUE
MANAGER

FIG.2

Figure 2 is block diagram showing the architecture of a search engine for actively indexing the World Wide Web according to one embodiment of Meadway's invention. Meadway, col. 3, ll. 33-35.

The system 200[5] includes (a) a central server 202 that stores a central index and processes search queries received over the Internet and (b) agent programs or agents 204 that reside on respective remote servers 208 and operate to provide periodic index updates to the central server 202. *Id.*, col. 3, ll. 35-40. The Examiner refers to remote servers 208 as "clients." Answer 7, 19.

Each agent 204 runs on a system, such as a web host server, at the site of an organization, and processes content (objects) for all web sites available via mass storage from that system. Meadway, col. 5, ll. 11-13. Agent 204 processes all web sites located within the mass storage area to which it has access, unless configured to exclude some portion of a site or sites. *Id.*, col. 5, ll. 14-16. Agent 204 reads files directly from local mass storage and indexes the keywords from the files and meta data about the files. *Id.*, col. 5, ll. 20-22.

Once the agent 204 has indexed the web sites at the remote server 208, the agent transmits a transaction list to the central server 202, which stores the transaction list on one of the agent update servers 222. *Id.*, col. 5, ll. 40-43. The transaction list, also referred to as a batch, contains a

[5] Reference numerals 200 and 202 do not appear in Figure 2.

series of deletion and addition transactions formatted as commands. *Id.*, col. 5, ll. 43-46. More specifically, each batch represents an incremental change record for the sites at the remote server 208 which is serviced by the agent 204. *Id.*, col. 5, ll. 46-48.

Meadway explains that "[t]he indexing process on each system may be initiated manually or on a scheduled basis, with updates transmitted whenever the user connects to the central service." *Id.*, col. 2, ll. 6-8.

The central server includes a number of agent update servers 222, each of which receives updates from the corresponding agent program and stores the current version of the agent program for download and updating of the local agent program. *Id.*, col. 4, ll. 13-16. In addition, each agent update server stores the digital signatures of the agent program and the remote server's (i.e., web host's) last local index, which are utilized during updating of the remote agent program and during updating of the local index. *Id.*, col. 4, ll. 16-20.

Central server 202 also includes a master index server RAID 218 (incorrectly numbered "128" in Figure 2) that contains a master copy of the entire central search index or catalog. *Id.*, col. 4, ll. 3-5. Each of the update servers 222 applies all index change transactions through a firewall/router 224 to the master index server 218 which, in turn, updates the central search index and then distributes those changes to the various index servers sets 216. *Id.*, col. 4, ll. 21-25.

We note that the Examiner characterizes the update information transmitted from a client to the central server as an "updated version" of the client's index. *See* Answer 17 ("Meadway disclosed when the central server receives an *updated version* of the client's index of shared data on a scheduled basis (Meadway, col. 2, lines 5-7) . . . . A particular pattern of activity is the client sending *updated versions* of the client's index on a scheduled basis.") (emphasis added).

The Examiner reads the step of "monitoring a peer-to-peer network for suspicious activity based on patterns of activity" on Welch, citing column 2, lines 35-43 (Answer 6), and reads the rest of the claim 1 limitations on Meadway. Specifically, the Examiner found that "[a] particular pattern of activity is the client sending updated versions of the client's index on a scheduled basis," citing column 2, lines 6-8 of Meadway. Answer 17.[6]

The Examiner further found that the step of "performing an action associated with a particular pattern when the particular pattern is detected" reads on the central server's updating of the central server's local index. *See* Answer 17 ("Meadway disclosed when the central server receives an updated version of the client's index of shared data on a scheduled basis (Meadway, col. 2, lines 5-7)[,] the central server performs updating the

[6] We assume that the Examiner misspoke in later stating that "[a]s explained above, the pattern of activity is the index of shared data at the peer." Answer 19.

central server's local index (Meadway, col. 4, lines 18-25)."). The "central server's local index" referred to by the Examiner is a copy, stored in an agent update server 222, of the remote web host's last local index. [7]

Appellants responded to the Examiner's reliance on Meadway with a number of arguments, none of which is persuasive. Regarding the second step of "performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network," Appellants argue that

> [i]n no way do [the cited] excerpts teach appellant's specific claim language, namely "performing an action associated with a particular pattern when the particular pattern is detected..." (emphasis added), especially when read in the context of the remaining claim language where "suspicious activity [is monitored] based on [the] patterns of activity" (emphasis added).

Reply Br. 6. To the extent this argument is based on the "suspicious activity" claim language, the argument is unconvincing for a number of reasons. First, Appellants have not supported their argument with a definition of "suspicious activity" that precludes that term from being read on Meadway's index update information. Second, the term "suspicious activity," which appears in the first ("monitoring") step of the claim, does not limit the second ("performing an action") step. That is, because the second step recites "a particular pattern" rather than "said pattern of

[7] The local index stored in agent update server 222 is also referred to
(Continued on next page.)

activity," it can be read on a pattern of activity other than the "patterns of activity" being monitored for suspicious activity in the first step. As a result, the first step can be read on, for example, Welch's disclosure of using the CME (connection management engine) 83 (Welch, col. 4, l. 55) to determine which stations are violating their security privileges (*id.* at col. 5, ll. 17-21), whereas the second step can be read on Meadway's central server's performance of the function of updating of its local index (in agent update server 222).

To the extent Appellants' above-quoted argument is based on the requirement that the action that is performed be "associated with" the particular pattern, we are also unpersuaded. Although Appellants (Reply Br. 6) disagree with the Examiner's construction of that claim language as broad enough to mean "[i]f something occurs, do something" (Answer 17), Appellants have not demonstrated that the Examiner's interpretation of "associated with" is unreasonable. Nor have Appellants shown that the Examiner erred in reading the term "particular pattern" on the client's transmission of index update information to central server 202.

Appellants also question the Examiner's finding (Answer 7) that "Meadway disclosed that the central server receives an updated version of the client's index of shared data on *a scheduled basis* (Meadway, col. 2, lines 5-7)." Reply Br. 8 (emphasis added). Specifically, Appellants argue that the

---

as a "remote local index." Meadway, col. 10, ll. 29-31.

"scheduled basis" described by Meadway refers to the indexing operations performed by the client at the remote server rather than to the client's transmission of updated index information to the central server. *See id.* ("Meadway discloses that the indexing process may be initiated manually or on a scheduled basis, not that the updates are transmitted on a scheduled basis as asserted by the Examiner. In contrast to the Examiner's arguments, Meadway discloses that updates are transmitted whenever the user connects to the central service."). We agree with Appellants that the cited passage in Meadway applies the term "scheduled basis" only to the *indexing* operation performed by agents 204 and that the Examiner therefore erred in finding that that term applies to the *transmission of index updates* from agents 204 to central server 202. However, this error has not been shown to constitute reversible error. Appellants have not demonstrated that the claim language "particular pattern [of activity]" cannot reasonably be read on an agent's connection to the central server, followed by transmission of client index update information to the central server.

For the foregoing reasons, Appellants have not shown that the Examiner reversibly erred in finding that the step of "performing an action associated with a particular pattern when the particular pattern is detected" reads on Meadway's updating of the master index in response to the transmitted index update information. As a result, it is unnecessary to address the Examiner's alternative reliance on Welch for that step. Answer 18.

Regarding the first "wherein" clause, which specifies that "the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network," Appellants argue:

> [T]he Examiner has attempted to interpret appellant's claimed peer-to-peer network to refer to, for example, any client and server communications. Appellant respectfully disagrees with this interpretation, especially in view of the previous amendments which require that "the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network."

Reply Br. 5. This argument is unpersuasive because it is not supported by an explanation of why Meadway fails to satisfy the claim language.

Appellants also argue that Meadway fails to satisfy the second and third "wherein" clauses. The second "wherein" clause specifies that "the pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data." The third "wherein" clause specifies that "monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline." The Examiner address these two "wherein" clauses as follows:

> As disclosed in Meadway, what is reported to the central server are the identities of the files on the client's computer that have been authorized for sharing with other clients on the network (Meadway, col. 2, lines 35-40). The whole purpose of reporting

> an updated index to the central server is to keep track of which peer is sharing which files and to direct requests for certain files to the correct peer (Meadway, col. 1, lines 47-52). One of ordinary skill in the art would interpret peers selecting which files they want to share with the network as *authorizing or permitting* which files are shared with other peers on the network. Therefore, *the index provides a baseline of authorized shares and permissions of files that will be provided if requested by others*, and when the central server receives an updated index, the central server evaluates a change in the authorized shared data and makes updates to the central server's local index.

Answer 19 (emphasis added).

In view of the Examiner's above-quoted statement that "the index provides a baseline of authorized shares and permissions of files that will be provided if requested by others," we understand the Examiner to be reading the second "wherein" clause (reciting a "configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions") on the client index at the remote server rather than on the transmitted index update information, on which the Examiner instead reads the recited "particular pattern [of activity]." This position of the Examiner is, in our opinion, consistent with the fact that the "particular pattern [of activity]" is recited as being "defined in terms of" the "configuration establishing a baseline of authorized shares and permissions." This "defined in terms of" terminology is broad enough to permit the "particular pattern [of activity]" (i.e., Meadway's transmission of index update information from the client to the central server) to represent updates to the

"configuration establishing a baseline of authorized shares and permissions" (i.e., the client index).

Regarding the second "wherein" clause, Appellants argue that the indexed information relates to the "contents of the files" and thus does not represent "a baseline of authorized shares and permissions." Reply Br. 7. To the extent Appellants are relying on the "authorized shares" claim language, the argument is unpersuasive because, as explained by the Examiner, the client index identifies files that the corresponding remote server 208 is authorized to share with others. As for the "authorized . . . permissions" claim language, Appellants have not explained how "permissions" differs from "shares" or why "authorized shares and permissions" cannot reasonably be read on the client index update information. Nor have Appellants explained why the term "baseline" cannot reasonably be read on the client index.

Turning now to the third "wherein" clause, as noted above the Examiner reads this clause on the central server's updating of its local index in response to the index update information received from a client. Appellants argue that

> the mere disclosure in Meadway that index "updates [are] transmitted whenever the user connects to the central service" fails to disclose a technique "wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline" (emphasis added), as claimed by appellant.

Reply Br. 8 (brackets in original). This argument is unconvincing because (1) it is not responsive to the Examiner's position, which is that the third "wherein" clause reads on how the central server responds to the index update information, and (2) Appellants have not explained why the underscored claim language cannot be reasonably read on the central server's response to the index update information.

In view of Appellants' failure to show reversible error in the Examiner's rejection of claim 1, we are affirming the rejection of that claim and the rejection of the other Issue 2/Group #1 claims, i.e., independent claims 15 and 29 and dependent claims 2, 16, and 30.

B. Issue 2/Group #2 (Claims 5, 19, and 33)

Of the claims in this group, we select claim 5 for consideration. That claim reads:

> 5. The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

We note that because this claim recites "a pattern of activity" without specifying that that term refers to the "patterns of activity" recited in the first step of claim 1 or to the "particular pattern" recited in the second step of claim 1, claim 5 does not further restrict those terms in claim 1.

The Examiner found that "in Welch, the two peers that are transmitting files (Welch, col. 5, lines 60-67) must be following a specific protocol in order for successful communication. Therefore, monitoring this

file transfer would require monitoring a specific protocol." Answer 20.

Appellants argue that

> Welch merely discloses [in the lines cited by the Examiner] that "[f]or each file transfer record 91, AME 81 notes the identity of the two stations involved in the file transfer using peer A pointer field 91a and peer B pointer field 91 b." Clearly, the mere disclosure of two stations involved in a file transfer completely fails to even suggest a "pattern of activity [that] is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol" (emphasis added), as claimed by appellant.

Reply Br. 9-10 (brackets in original). This argument is unpersuasive because it fails to address the Examiner's finding that the peers in Welch's network are necessarily using the same protocol. Also, Appellants have not explained how the claim terms underscored above should be construed or why those claim terms thus construed fail to read on Welch considered alone or in combination with Meadway.

We are therefore affirming the rejection of claims 5, 19, and 33.

C. Issue 2/Group #3 (Claims 11, 25, and 39)

From this group, we select claim 11 for consideration. That claim reads:

> 11. The computerized method of claim 1, wherein the patterns of activity are local to a peer in the peer-to-peer network.

The Examiner found that "by Welch disclosing monitoring file transfers from peer A to peer B (Welch, col. 5, lines 58-67) includes [*sic*; Welch

discloses] monitoring patterns of activity that are local to the peer." Answer 21. Appellants argue that

> Welch merely discloses, in item 114 of Fig. 5, that if "this [is] an open file request" then item 116, of Fig. 5, "create[s] a record of this connection in database." Clearly, monitoring for open file requests between peer stations fails to even suggest a technique "wherein the patterns of activity are local to a peer in the peer-to-peer network" (emphasis added), as claimed by appellant.

Reply Br. 10 (brackets in original). This argument is unpersuasive because the Examiner does not rely on Welch's discussion of "open file requests," which appears in column 5, lines 54-57. The Examiner instead relies on lines 58-67 of that column, which do not discuss open file requests.

The rejection of claims 11, 25, and 39 is therefore affirmed.

D. Issue 2/Group #4 (Claim 45)

Claim 45 reads:

> 45. The computerized method of claim 1, wherein a share configuration loop is executed to detect changes to shares and corresponding permissions, and take action as a function of a type of the changes.

The Examiner found that this claim language reads on Meadway because "Meadway disclosed that when the central server receives an updated version of the client's index of shared data on a scheduled basis (Meadway, col. 2, lines 5-7), the central server performs updating the

changes in the central server's local index (Meadway, col. 4, lines 18-25)."

Answer 21. Appellants argue that

> merely transmitting updates whenever the user connects to the central service, and having the update servers apply all index change transactions to the master index server, fails to even suggest a technique "wherein a share configuration loop is executed to detect changes to shares and corresponding permissions, and take an action as a function of a type of the changes" (emphasis added), as claimed by appellant.

Reply Br. 12. This argument is unpersuasive because Appellants have not explained how the underscored claim language should be construed or why that language thus construed is not disclosed or suggested by Meadway. Furthermore, to the extent Appellants are arguing that Meadway fails to describe the agent update servers 222 in the central server as employing a "share configuration loop," we conclude that it would have been obvious to use a loop to detect receipt of index update information from a client and to update the agent update server's local index. Because the index update information related to files to be shared by the clients, it would be accurate characterize such a loop as a "share configuration loop."

The rejection of claim 45 is therefore affirmed.

E. Issue 2/Group #5 (Claim 46)

Claim 46 reads:

> 46. The computerized method of claim 45, wherein the share configuration loop is executed dynamically.

The Examiner construed the phrase "executed dynamically" to mean "an action that is performed when or as needed while a program is running" (Answer 21) and found:

> One of ordinary skill in the art would interpret the programs running on the central server of Meadway to dynamically update the records of its local index when receiving an updated index from the client. . . . Whenever an agent sends an updated index to the central server, the central server updates its local index.

Id. at 22.

Appellants' argument that "[s]imply nowhere in Meadway is there even any mention of a 'share configuration loop [that] is executed dynamically,' as claimed by appellant (emphasis added)" (Reply Br. 12), is unpersuasive for the reasons given above in the discussion of claim 45, to which we would add that use of a loop is inherently a dynamic operation.

The rejection of claim 46 is therefore affirmed.

F. Issue 2/Group #6 (Claim 47)

Claim 47 reads:

> 47. The computerized method of claim 45, wherein the share configuration loop is executed on a schedule.

The Examiner found that Meadway satisfies this claim because "[e]very time an updated index is received, the central server updates its local index." Answer 22. Appellants (Reply Br. 13) have not explained why the term "schedule" does not read on this disclosure in Meadway.

The rejection of claim 47 is therefore affirmed.

G. Issue 2/Group #7 (Claim 48)

Claim 48 reads:

> The computerized method of claim 45, wherein the share configuration loop examines a current shared configuration against a previously recorded shared configuration.

The Examiner explained that

> when the central server receives an updated version of the client's index of shared data (Meadway, col. 2, lines 5-7)[,] the central server performs updating the central server's local index (Meadway, col. 4, lines 18-25). In order for central server to make the proper changes, the client's updated index is examined against the central server's local index (previously recorded share configuration).

Answer 23. Appellants responded that

> Meadway discloses that "the update servers store the digital signature of the agent program and also store the remote web hosts' last local index, which are utilized during the updating of the remote agent program and during updating the local index" (emphasis added). Appellant asserts that the mere disclosure that the update servers utilize the last local index during updating the local index fails to suggest a technique "wherein the share configuration loop examines a current share configuration against a previously recorded shared configuration" (emphasis added), as claimed by appellant.

Reply Br. 14. Appellants appear to be arguing that Meadway's update servers 222 do not include share configuration loops. For the reasons given

above in the discussion of claim 45, it would have been obvious to employ share configuration loops in the update servers.

The rejection of claim 48 is affirmed.

H. Issue 2/Group #8 (claim 49)

Claims 49 reads:

> 49. The computerized method of claim 45, wherein, if the change includes an attempt to un-share a file or directory, the action includes a log entry.

The Examiner found that this claim language is inherently satisfied because

> any change in the peer's local index, regarding what files are shared or not shared by the peer, is included in the updated index that is sent to the central server, and the central server updates its local index (Meadway, col. 1, lines 45-50, col. 2, lines 1-10, 35-40). The local index of the central server is a log of the files permitted for sharing by each peer.

Answer 23 (underlining omitted). Appellants argue that

> the excerpts Meadway relied upon by the Examiner fail to disclose an "action includ[ing] a log entry" resulting from a "change includ[ing] an attempt to un-share a file or directory." Also, appellant asserts that the Examiner's statement that the "local index of the central server is a log of the files permitted for sharing by each peer" improperly equates an index with a log.

Reply Br. 15 (brackets in original). This argument is unconvincing because it is not supported by any evidence that the broadest reasonable interpretation of "log" precludes it from being read on Meadway's local index. The Examiner also correctly found that this claim's requirement for a

log entry if there is an attempt to "un-share" a file or directory is satisfied because Meadway's local index reflects sharing and unsharing of files.

The rejection of claim 49 is affirmed.

THE § 103 REJECTION (ISSUE 3) BASED ON WELCH IN VIEW OF MEADWAY AND CONKLIN

Conklin discloses a system for systematic monitoring, intrusion identification, notification, and tracking of unauthorized activities, such as methods or systems used by "hackers" to intrude into computer networks. Conklin, col. 1, ll. 11-14.

A. Issue 3/Group #1 (claims 4, 10, 12, 18, 24, 26, 32, 38, and 40-42)

Because Appellants treat this group of claims as standing or falling with the Issue 2/Group #1 claims (Reply Br. 16), we are affirming the § 103(a) rejection of the Issue 1/Group # 1 claims for the same reasons that we affirmed the § 103(a) rejection of the Issue 2/Group # 1 claims.

B. Issue 3/Group # 2 (claims 7, 21, and 35)

Of these claims, we select claim 7 for consideration.

Claim 7 reads:

> 7. The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address.

The Examiner found that

> Conklin disclosed identifying the traffic as reportable activity indicating source and destination address of the packet (Conklin, col. 5, lines 25-35). Since Conklin identifies intrusions into the network from an external source, Conklin disclosed reporting patterns of activity that is defined in terms of network traffic having a foreign address.

Answer 24-25 (bolding and underlining omitted). The cited lines state in relevant part:

> When a packet or accumulation of packets match a predefined intrusion profile the Intrusion Detection function identifies the network traffic as a reportable activity [and] will construct a data structure which contains a date/time stamp indicating the time of detection, the source and destination Internet Protocol (IP) addresses, an assigned message identifying the event detected.

Conklin, col. 5, ll. 24-31. Regarding the above-quoted passage, we agree with Appellants' argument "the pattern of activity in Conklin is not taught to be 'defined in terms of network traffic . . . having a foreign address,' as claimed by appellant, but instead only general source and destination addresses are reported after the match is made." Reply Br. 17 (underlining omitted).

However, Appellants' argument fails to address Conklin's additional disclosure that

> network specific characteristics or facts may be developed from the network data collection over time and stored in the . . . database. For example, certain network traffic facts or characteristics can become measurably predictable such as time of day, number and types of packets, *common destination/ source address combinations*, etc. . . . If network traffic is

> deemed outside of normal tolerances for measured characteristics, then the Intrusion Detection will activate the Alert Notification, Evidence Logging, and Incident Analyzer Reporter, functions as described below.

Conklin, col. 4, l. 61 to col. 5, l. 9 (emphasis added). It would appear that in the event that the normal "common destination/source address combinations" do not include foreign addresses, the pattern of activity that would be detected would be the presence of a foreign address.

We are therefore affirming the rejection of claims 7, 21, and 35.

C. Issue 3/Group # 3 (claims 9, 23, and 37)

Of these claims, we select claim 9 for consideration.

Claim 9 reads:

> 9. The computerized method of claim 1, wherein the action comprises logging information about the particular pattern.

The Examiner found that "if the packet is detected as being part of a particular pattern, and the entire packets is written to a log file (Conklin, col. 5, lines 33-36), then this must contain information regarding the particular pattern, since the packet is what caused the detection in the first place." Answer 25 (underlining omitted). The lines in Conklin cited by the Examiner explain that "[w]hen a positive identification of a reportable activity occurs, the entire triggering packet(s) may be written to a log file created in the Evidence Logging function" (col. 5, ll. 33-36).

Appellants responded that "Conklin suggests writing the triggering packet(s) to the log file, and not information about the particular pattern that caused the trigger." Reply Br. 18. This argument is unconvincing because it fails to take into account Conklin's above-noted disclosure that the data structure that is recorded when a packet or accumulation of packets match a predefined intrusion profile includes "an assigned message identifying the event detected." Conklin, col. 5, ll. 30-31. Furthermore, Conklin explains that "the log file written is named using the date/time and name of [the] event detected." *Id.*, col. 5, ll. 37-39.

The rejection of claims 9, 23, and 37 is affirmed.

D. Issue 3/Group # 4 (claims 13, 27, and 43)

Of the claims in this group, we select claim 13 for consideration. Claim 13 reads:

> 13. The computerized method of claim 1 further comprising:
>
> obtaining a set of rules specifying the patterns of activity and associated actions.

The Examiner does not construe the "associated actions" in this claim as referring to the "action" recited in the "performing" step of claim 1, which step calls for "performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network" and which step the Examiner reads on Meadway's central server when it updates the local index in response to index update information. Instead, the Examiner reads

the recited "associated actions" of claim 13 on actions which are part of the "patterns of activity":

> [T]he limitation, "associated actions", in its broadest reasonable interpretation, could simply mean an action describing the pattern of activity, hence the pattern of activity. . . . Conklin disclosed obtaining pre-stored patterns of activity in a database (Conklin, col. 4, lines 45-67). One of ordinary skill in the art would interpret patterns of activity to include associated actions since a pattern of activity would require actions.

Answer 25 (underlining omitted). Thus, the Examiner is reading the recited "associated actions" on the actions that comprise the "particular pattern" rather than on actions taken in response to detection of the particular pattern.

Appellants responded by arguing that

> Conklin's actions of identifying, activating, and opening a data channel when collected data matches the database's stored data fails to meet and even *teaches away* from the need for "a set of rules specifying the patterns of activity and associated actions" (emphasis added), as claimed by appellant, since the actions are already defined for all data matches.

Reply Br. 19. This argument is unpersuasive because it is not responsive to the Examiner's position that the recited "associated actions" can be read on the actions that comprise the "particular pattern."

The rejection of claims 13, 27, and 43 is affirmed.

E. Issue 3/Group #5 (claims 14, 28, and 44)

We select claim 14 for consideration. Claim 14 reads:

> 14. The computerized method of claim 13 further comprising:
> refreshing the set of rules when the set of rules changes.

The Examiner stated that "Conklin disclosed that Intrusion Detection may incorporate algorithms or patterns to detect attempted intrusions or intrusions on the network[ ](Conklin, col. 4, lines 45-50), meaning that algorithms may be added to the Intrusion Detection system, thereby refreshing sets of rules to follow." Answer 26. The cited lines read as follows:

> Intrusion Detection may incorporate algorithms or patterns to detect attempted intrusions or intrusions on the network. As each packet of network data is passed from the Network Observation function, the Intrusion Detection function examines the data in comparison to a series of predefined or learned
> patterns which are pre-stored or developed from data received from the network.

Conklin, col. 4, ll. 45-50.

Appellants argue that "[s]imply disclosing that Intrusion Detection incorporates algorithms or patterns fails to even suggest 'refreshing the set of rules when the set of rules changes' (emphasis added), as claimed by appellant." Reply Br. 20. This argument is unconvincing for two reasons. First, even assuming the cited passage in Conklin fails to suggest that the algorithms or patterns can be added or changed, it would have been obvious

to permit such changes. Second, Conklin specifically discloses that "th[e] Intrusion Detection function may be modified to allow customized triggers to be entered by system administrators." Conklin, col. 5, ll. 10-12.

The rejection of claims 14, 28, and 44 is affirmed.

DECISION

The rejection of claims 1, 15, 29, and 45 stand rejected under 35 U.S.C. §112, second paragraph, for indefiniteness is reversed.

The rejection of claims 1, 2, 5, 11, 15, 16, 19, 25, 29, 30, 33, 39, and 45-49 under § 103(a) for obviousness over Welch in view of Meadway is affirmed.

The rejection of claims 4, 7, 9, 10, 12-14, 18, 21, 23, 24, 26-28, 32, 35, 37, 38, and 40-44 under § 103(a) for obviousness over Welch in view of Meadway and Conklin is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. §§ 41.50(f) and 41.52(b).

AFFIRMED

msc

ZILKA-KOTAB PC
PO BOX 721120
SAN JOSE, CA 95172-1120